



US009208041B2

(12) **United States Patent**
Bennah et al.

(10) **Patent No.:** **US 9,208,041 B2**
(45) **Date of Patent:** ***Dec. 8, 2015**

(54) **DYNAMIC PROTECTION OF A MASTER OPERATING SYSTEM IMAGE**

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION**,
Armonk, NY (US)

(72) Inventors: **Albert D. Bennah**, Cary, NC (US);
Robert A. Vrabel, Apex, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 137 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/645,914**

(22) Filed: **Oct. 5, 2012**

(65) **Prior Publication Data**

US 2014/0101429 A1 Apr. 10, 2014

(51) **Int. Cl.**
G06F 11/22 (2006.01)
G06F 9/445 (2006.01)

(52) **U.S. Cl.**
CPC **G06F 11/2289** (2013.01); **G06F 8/60**
(2013.01); **G06F 8/63** (2013.01)

(58) **Field of Classification Search**
CPC G06F 11/2289; G06F 8/63; G06F 8/60
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,272,626 B1 8/2001 Cobbett
6,330,715 B1 12/2001 Razzaghe-Ashrafi

6,513,115 B2 1/2003 Nock et al.
7,600,216 B2 10/2009 Shlomai
7,694,280 B2 4/2010 James et al.
7,757,214 B1 7/2010 Palczak et al.
7,802,246 B1 9/2010 Kennedy et al.
8,117,168 B1 2/2012 Stringham

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2012/048030 A2 4/2012

OTHER PUBLICATIONS

Zhang et al., CCOA: Cloud computing open architecture, [Online] 2009, Web Services, 2009. ICWS 2009. IEEE International Conference on, [Retrieved from the Internet] <<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5175875&isnumber=5175786>> pp. 607-616.*

(Continued)

Primary Examiner — Thuy Dao

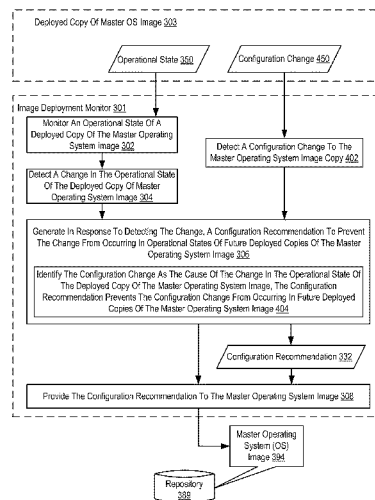
Assistant Examiner — Ravi K Sinha

(74) *Attorney, Agent, or Firm* — Edward J. Lenart; James R. Nock; Kennedy Lenart Spraggins LLP

(57) **ABSTRACT**

Methods, apparatuses, and computer program products for dynamic protection of a master operating system image are provided. Embodiments include monitoring, by an image deployment monitor, an operational state of a deployed copy of a master operating system (OS) image; detecting, by the image deployment monitor, a change in the operational state of the deployed copy of the master OS image; in response to detecting the change, generating, by the image deployment monitor, a configuration recommendation to prevent the change from occurring in operational states of future deployed copies of the master OS image; and providing, by the image deployment monitor, the configuration recommendation to the master OS image.

9 Claims, 4 Drawing Sheets



(56)

References Cited

U.S. PATENT DOCUMENTS

- 8,181,174 B2 * 5/2012 Liu 718/1
8,219,983 B1 * 7/2012 Sobel et al. 717/168
8,239,509 B2 * 8/2012 Ferris et al. 709/223
8,296,251 B1 * 10/2012 Athayde 706/45
8,347,280 B2 1/2013 Swarna
8,352,608 B1 * 1/2013 Keagy et al. 709/226
8,381,191 B2 2/2013 Mondal
8,423,958 B2 4/2013 Velupillai
8,612,566 B2 * 12/2013 Ferris et al. 709/223
8,627,293 B2 1/2014 Perrone et al.
8,635,686 B2 1/2014 Sriram
8,869,135 B1 10/2014 Fitzgerald et al.
2003/0051128 A1 * 3/2003 Rodriguez et al. 713/100
2004/0025154 A1 2/2004 Sedlack
2004/0153478 A1 8/2004 Igouchkine
2004/0162876 A1 8/2004 Kohavi
2004/0181776 A1 9/2004 Atkin et al.
2004/0230731 A1 * 11/2004 Arimilli et al. 710/302
2005/0235352 A1 10/2005 Staats et al.
2006/0161895 A1 7/2006 Speeter et al.
2006/0184937 A1 8/2006 Abels et al.
2006/0248139 A1 11/2006 Sundar
2006/0248513 A1 11/2006 Foster et al.
2007/0180509 A1 8/2007 Swartz et al.
2007/0226358 A1 9/2007 Krywaniuk
2007/0283324 A1 12/2007 Geisinger
2007/0283329 A1 12/2007 Caprihan et al.
2008/0052675 A1 2/2008 Wookey
2008/0098379 A1 4/2008 Newman et al.
2008/0104573 A1 5/2008 Singla et al.
2008/0141010 A1 * 6/2008 Crowell et al. 712/226
2008/0141217 A1 6/2008 Goetz et al.
2008/0155534 A1 6/2008 Boss et al.
2008/0184200 A1 * 7/2008 Burns et al. 717/121
2009/0016220 A1 * 1/2009 Uysal et al. 370/232
2009/0019438 A1 1/2009 Madduri et al.
2009/0019535 A1 1/2009 Mishra et al.
2009/0037680 A1 2/2009 Colbert et al.
2009/0048993 A1 2/2009 Lohrbach et al.
2009/0089624 A1 4/2009 Austen et al.
2009/0100420 A1 4/2009 Sapuntzakis et al.
2009/0118839 A1 5/2009 Accapadi et al.
2009/0228868 A1 9/2009 Drukman et al.
2009/0265707 A1 * 10/2009 Goodman et al. 718/1
2009/0300057 A1 * 12/2009 Friedman 707/102
2009/0300149 A1 * 12/2009 Ferris et al. 709/222
2009/0300151 A1 * 12/2009 Friedman et al. 709/222
2009/0300607 A1 12/2009 Ferris et al.
2009/0300641 A1 * 12/2009 Friedman et al. 718/104
2009/0300707 A1 12/2009 Garimella et al.
2010/0037207 A1 2/2010 Chambers et al.
2010/0153443 A1 6/2010 Gaffga et al.
2010/0192143 A1 * 7/2010 Ingle et al. 717/172
2010/0229175 A1 9/2010 Gonzalez et al.
2010/0257523 A1 * 10/2010 Frank 718/1
2010/0274890 A1 10/2010 Patel et al.
2010/0325410 A1 * 12/2010 Fitzgerald et al. 713/2
2010/0332637 A1 12/2010 Doi et al.
2010/0332890 A1 12/2010 Chen et al.
2011/0016414 A1 * 1/2011 Ernst et al. 715/764
2011/0126168 A1 5/2011 Ilyayev
2011/0131301 A1 6/2011 Klein et al.
2011/0145789 A1 6/2011 Rasch et al.
2011/0154320 A1 * 6/2011 Verma 718/1
2011/0161952 A1 6/2011 Poddar et al.
2011/0173605 A1 7/2011 Bourne
2012/0030459 A1 2/2012 Aldridge et al.
2012/0030672 A1 2/2012 Zygmuntowicz et al.
2012/0054868 A1 3/2012 Ramalingam
2012/0079474 A1 3/2012 Gold et al.
2012/0084414 A1 * 4/2012 Brock et al. 709/221
2012/0084752 A1 * 4/2012 Arnold et al. 717/121
2012/0102160 A1 * 4/2012 Breh et al. 709/220
2012/0102481 A1 * 4/2012 Mani et al. 717/172
2012/0131577 A1 5/2012 Arcese et al.
2012/0159471 A1 6/2012 de Souza et al.
2012/0167048 A1 6/2012 Walsh et al.
2012/0246619 A1 9/2012 Thirumalai et al.
2012/0278797 A1 * 11/2012 Secrist et al. 717/176
2012/0284405 A1 * 11/2012 Ferris et al. 709/224
2013/0067049 A1 3/2013 Ghosh et al.
2013/0080619 A1 3/2013 Assuncao et al.
2013/0080997 A1 * 3/2013 Dattathreya 717/121
2013/0125107 A1 5/2013 Bandakka et al.
2013/0138718 A1 5/2013 Mallur et al.
2013/0332921 A1 * 12/2013 Khutornenko et al. 718/1
2014/0033188 A1 1/2014 Beavers et al.
2014/0033189 A1 * 1/2014 Buswell 717/170
2014/0040438 A1 * 2/2014 Donahue et al. 709/220
2014/0052683 A1 2/2014 Kirkham et al.
2014/0075172 A1 * 3/2014 Knichel et al. 713/2
2014/0101421 A1 4/2014 Bennah et al.
2014/0101422 A1 4/2014 Bennah et al.
2014/0101428 A1 4/2014 Bennah et al.
2014/0101430 A1 4/2014 Bennah et al.
2014/0101431 A1 4/2014 Bennah et al.
2014/0108774 A1 4/2014 Bennah et al.
2014/0108779 A1 * 4/2014 Bennah et al. 713/100
2014/0108951 A1 4/2014 Dharawat et al.
2014/0157056 A1 * 6/2014 Bennah et al. 714/37

OTHER PUBLICATIONS

- Carl A. Waldspurger, Memory resource management in VMware ESX server, [Online] 2002, SIGOPS Oper. Syst. Rev. 36, SI (Dec. 2002), [Retrieved from the Internet] <<http://doi.acm.org/10.1145/844128.844146>> pp. 181-194.*
Badger et al., Draft cloud computing synopsis and recommendations, [Online] 2011, NIST special publication 800-146 2011, [Retrieved from the Internet] <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.3178&rep=rep1&type=pdf>> 84 pages.*
Choi, H., et al., "Autonomous Learning for Efficient Resource Utilization of Dynamic VM Migration", ICS'08, Jun. 2008, pp. 185-194, ACM, USA.
Venners, B., "Inside the Java Virtual Machine", Chapter 5 of Inside the Java Virtual Machine, www.artima.com (online), [accessed Jul. 6, 2012], 1-53 pp., URL: <http://www.artima.com/insidejvm/ed2/jvmP.html>.
Hudson, "Hyper-V Virtual Machine (VM) Parent-Child Configuration Using Differencing Disks", Microsoft TechNet Article, Sep. 2010, [accessed Aug. 7, 2012], 2 pp., URL: <http://social.technet.microsoft.com/wiki/contents/articles/1393.hyper-v-virtual-machine-vm-parent-child-configuration-using-differencing-disks.aspx>.
"vSphere 5: Updating/Installing profile or vib using esxcli", virtualvm.info (online), May 2012, [accessed Aug. 7, 2012], 3 pp., URL: <http://virtualvm.info/?p=170>.
Office Action, U.S. Appl. No. 13/645,808, filed Jul. 24, 2014, pp. 1-12.
Office Action, U.S. Appl. No. 13/646,020, filed May 23, 2014, pp. 1-16.
Office Action, U.S. Appl. No. 13/653,090, filed May 30, 2014, pp. 1-25.
Office Action, U.S. Appl. No. 13/658,937, May 21, 2014, pp. 1-21.
Oasysadmin, "Copying, moving and replicating the MDT 2010 deployment share", Nov. 2011, pp. 1-9, oasysadmin.com (online), URL: oasysadmin.com/2011/11/03/copying-moving-and-replicating-the-mdt-2010-deployment-share/.
Bell et al., "Configuration Description, Deployment, and Lifecycle Management (CDDL) Foundation Document", GFD.50, Aug. 2005, 37 pages, Global Grid Forum (online), URL: www.ogf.org/documents/GFD.50.pdf.
Rasmussen et al., "Managing WebSphere DataPower Device configurations for high availability, consistency, and control, Part 2: Application promotion strategies", IBM developerWorks, WebSphere Technical Library, Apr. 2009, 15 pages, IBM developerWorks (online), URL: www.ibm.com/developerworks/websphere/library/techarticles/0904_rasmussen/0904_rasmussen.html.

(56)

References Cited

OTHER PUBLICATIONS

White, "How to Deploy Entire Systems in Mac OS X 10.5", chapter from Apple Training Series: Mac OS X Deployment v10.5, peachpit.com (online), Aug. 20, 2008, pp. 1-9, Pearson Education, Peachpit Press, San Francisco, CA, USA.

Wentzlaff et al., "An Operating System for Multicore and Clouds: Mechanisms and Implementation", Proceedings of the 1st ACM Symposium on Cloud Computing (SoCC'10), Jun. 2010, pp. 1-10, ACM New York, NY, USA.

Scarfone et al., "Guide to Security for Full Virtualization Technologies", Jan. 2011, 35 pages, National Institute of Standards and Technology, Gaithersburg, MD, USA.

* cited by examiner

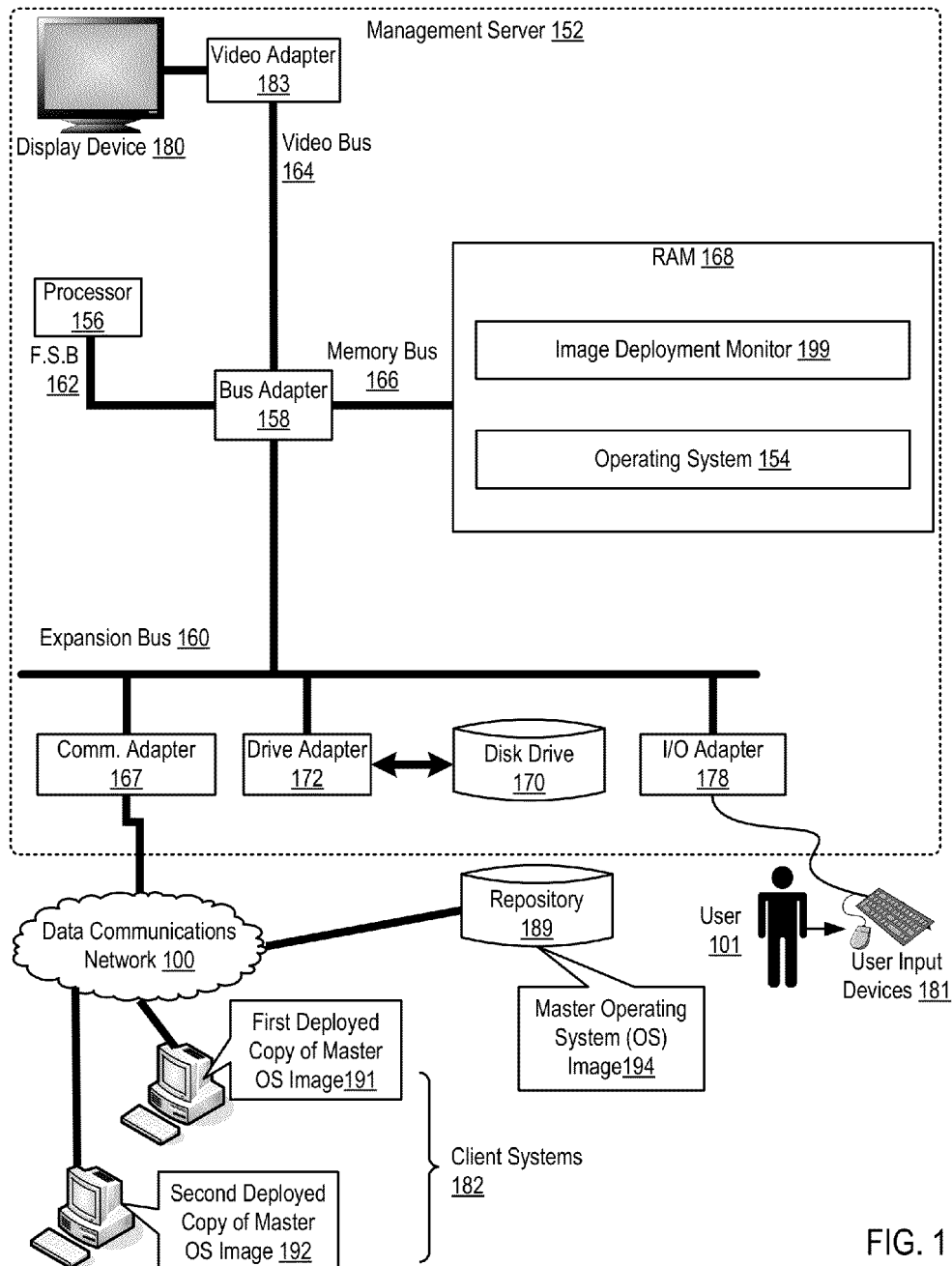


FIG. 1

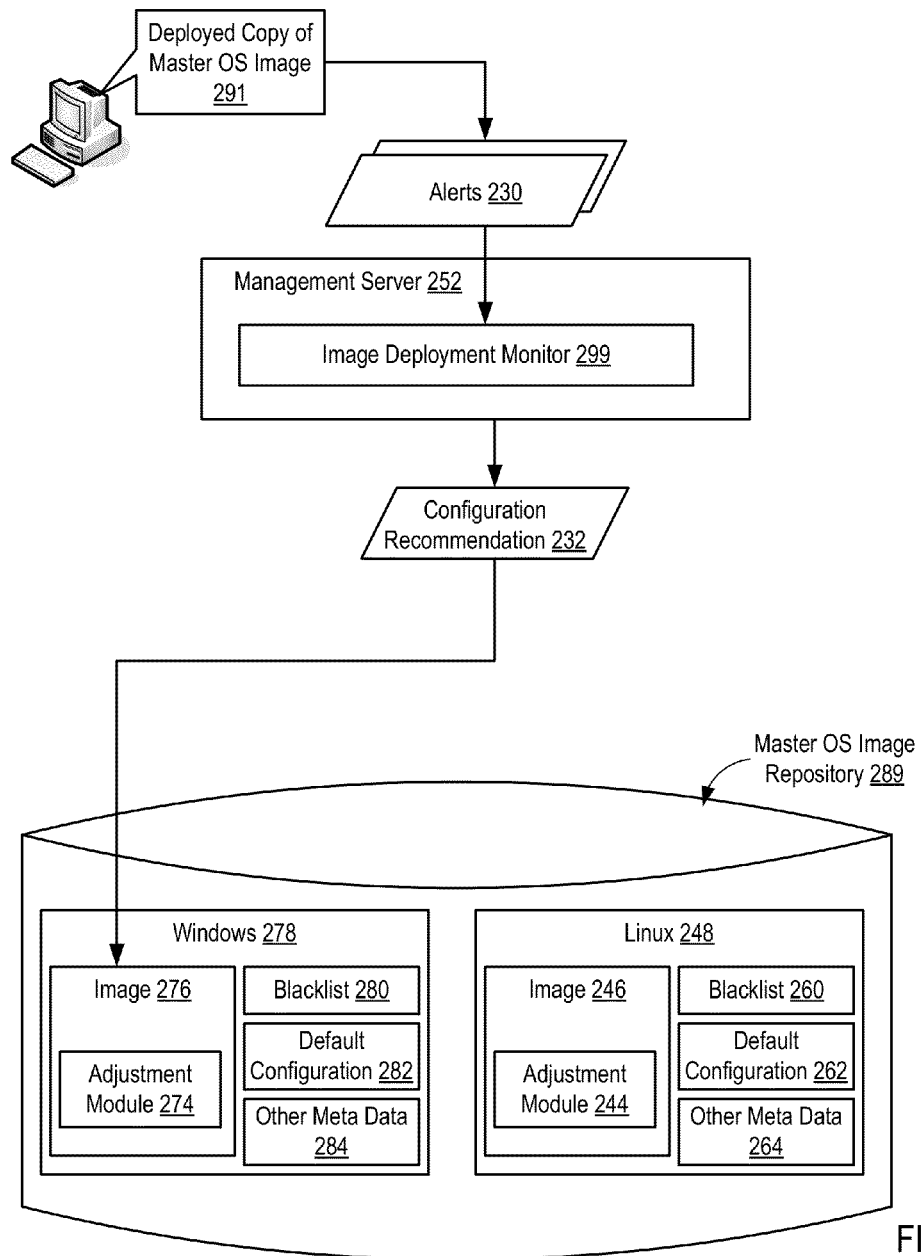


FIG. 2

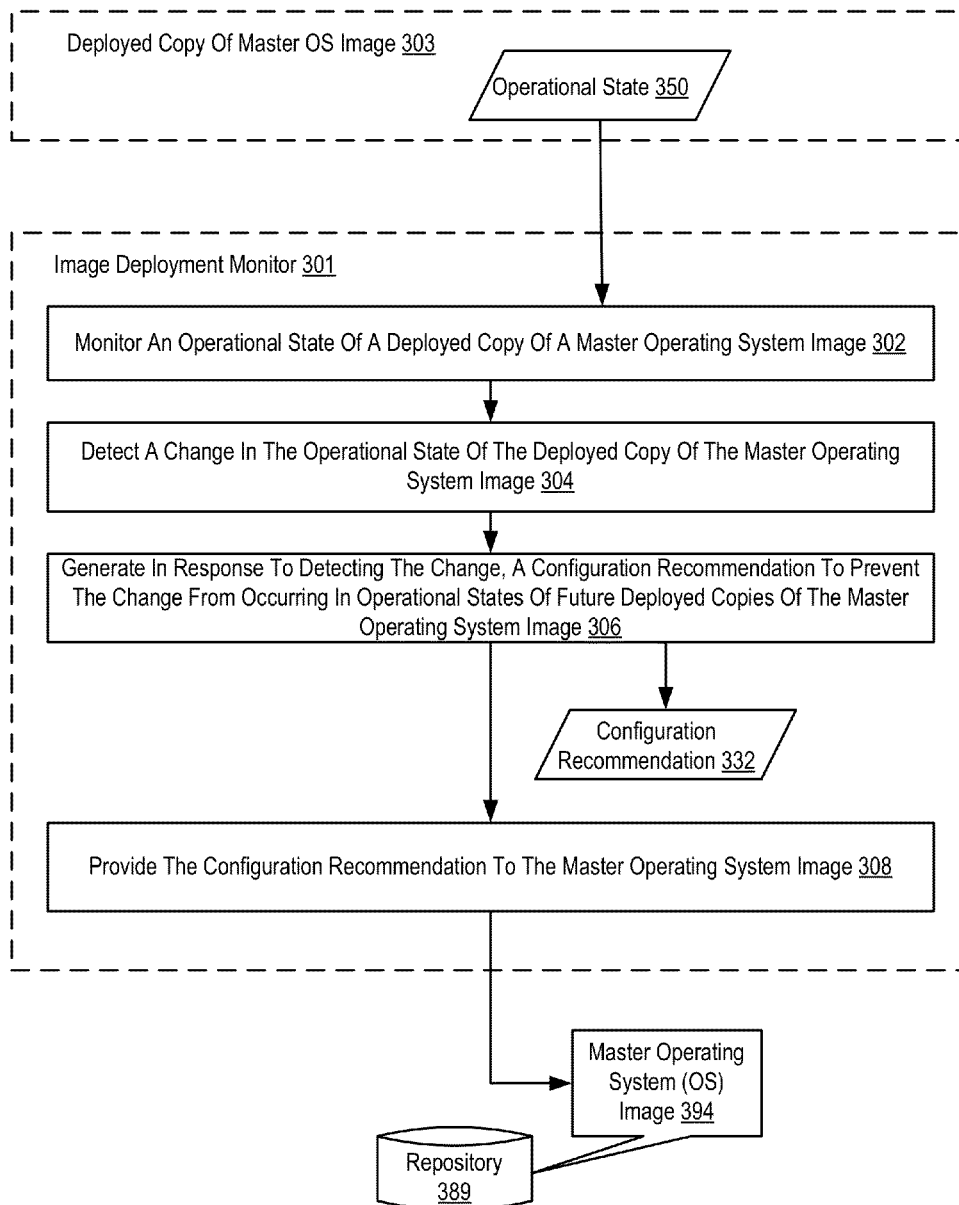


FIG. 3

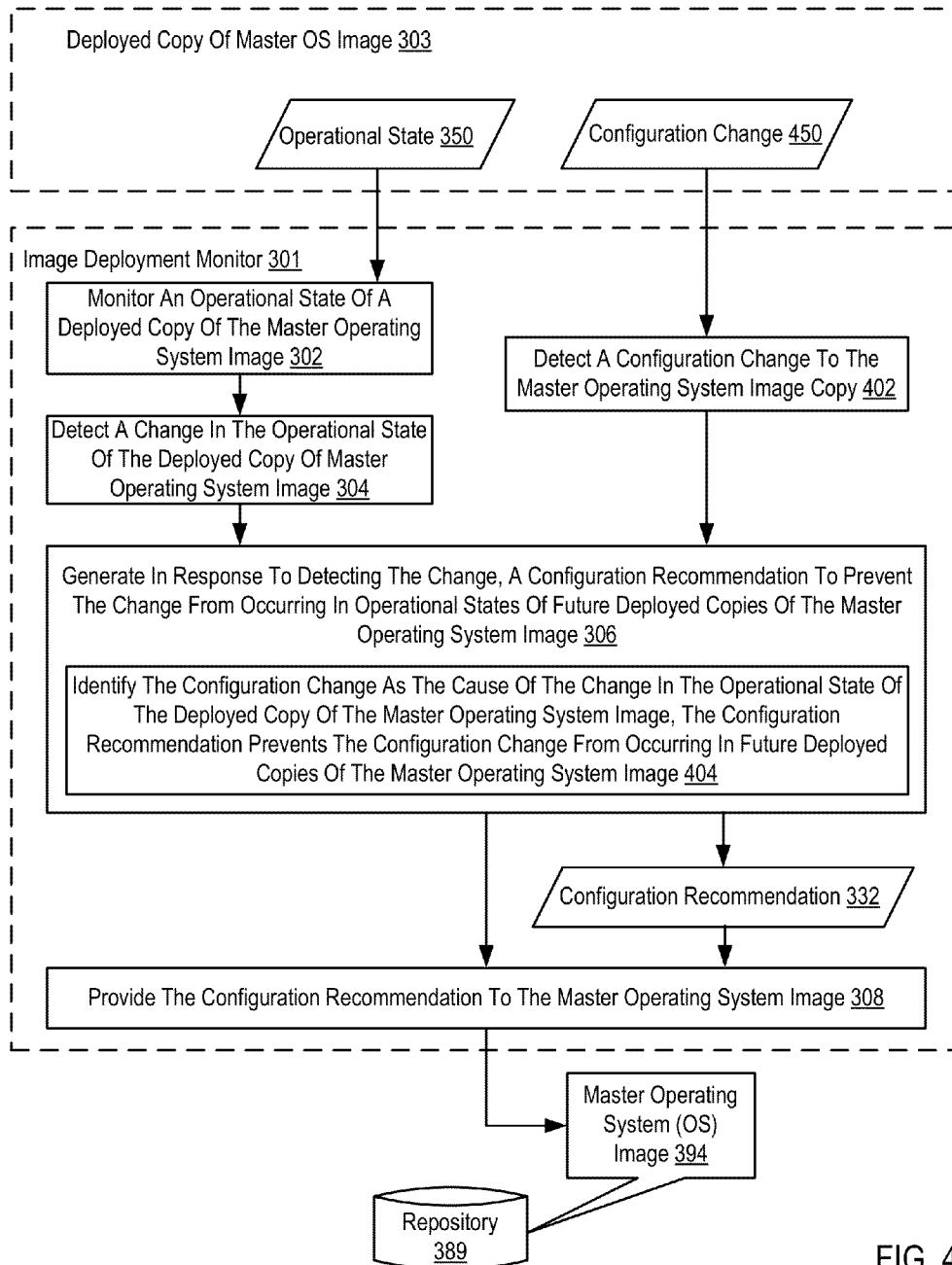


FIG. 4

1

DYNAMIC PROTECTION OF A MASTER OPERATING SYSTEM IMAGE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The field of the invention is data processing, or, more specifically, methods, apparatuses, and computer program products for dynamic protection of a master operating system image.

2. Description of Related Art

In modern data centers, system administrators often maintain a collection of master operating system (OS) images that are reserved for deployment unto new systems as these systems become operational. A master OS image is a boot device image that includes a representation of a computer program and its related data such as a kernel, file system, and libraries at a particular given point in time. Master OS images or "Golden" master OS images imply a degree of trust and stability based on prior quality assessments performed against them. After creating a master OS image, threats may arise that challenge the integrity of the configuration of the master OS image.

SUMMARY OF THE INVENTION

Methods, apparatuses, and computer program products for dynamic protection of a master operating system image are provided. Embodiments include monitoring, by an image deployment monitor, an operational state of a deployed copy of a master operating system (OS) image; detecting, by the image deployment monitor, a change in the operational state of the deployed copy of the master OS image; in response to detecting the change, generating, by the image deployment monitor, a configuration recommendation to prevent the change from occurring in operational states of future deployed copies of the master OS image; and providing, by the image deployment monitor, the configuration recommendation to the master OS image.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular descriptions of exemplary embodiments of the invention as illustrated in the accompanying drawings wherein like reference numbers generally represent like parts of exemplary embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 sets forth a block diagram of automated computing machinery comprising an exemplary management server useful in dynamic protection of a master operating system image according to embodiments of the present invention.

FIG. 2 sets forth a block diagram of a system comprising another example management server useful in dynamic protection of a master operating system image according to embodiments of the present invention.

FIG. 3 sets forth a flow chart illustrating an exemplary method for dynamic protection of a master operating system image according to embodiments of the present invention.

FIG. 4 sets forth a flow chart illustrating a further exemplary method for dynamic protection of a master operating system image according to embodiments of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Exemplary methods, apparatuses, and computer program products for dynamic protection of a master operating system

2

image in accordance with the present invention are described with reference to the accompanying drawings, beginning with FIG. 1. Dynamic protection of a master operating system image in accordance with the present invention is generally implemented with computers, that is, with automated computing machinery. For further explanation, therefore, FIG. 1 sets forth a block diagram of automated computing machinery comprising an exemplary management server (152) useful in dynamic protection of a master operating system image according to embodiments of the present invention. The management server (152) of FIG. 1 includes at least one computer processor (156) or 'CPU' as well as random access memory (168) ('RAM') which is connected through a high speed memory bus (166) and bus adapter (158) to processor (156) and to other components of the management server (152).

Stored in RAM (168) is an image deployment monitor (199) that includes computer program instructions for dynamic protection of a master operating system image according to embodiments of the present invention. Specifically, the image deployment monitor (199) includes computer program instructions that when executed by the computer processor (156) cause the image deployment monitor (199) to carry out the step of monitoring an operational state of a deployed copy of a master operating system (OS) image. In the example of FIG. 1, the management server (152) is configured to monitor deployed copies (191, 192) on client systems (182) where the original master OS image (194), from which the copies (191, 192) were deployed, resides within a repository (189).

The image deployment monitor (199) also includes computer program instructions that when executed by the computer processor (156) cause the image deployment monitor (199) to carry out the step of detecting a change in the operational state of the deployed copy (191, 192) of the master OS image (194). An operational state of a deployed copy may be any type of monitorable characteristics related to the deployed copy, such as a physical state of the system upon which the copy is deployed; server performance; network performance; and security. Examples of changes in the operational state of a deployed copy include system errors or component failures, such as a failure to communicate with a peripheral device.

The image deployment monitor (199) also includes computer program instructions that when executed by the computer processor (156) cause the image deployment monitor (199) to carry out the steps of generating in response to detecting the change, a configuration recommendation to prevent the change from occurring in operational states of future deployed copies of the master OS image; and providing, by the image deployment monitor, the configuration recommendation to the master OS image.

By using a configuration recommendation to prevent a change detected in a deployed copy of a master OS image (194), from occurring in a future deployed copy, the image deployment monitor (199) may protect the master OS image (194) against threats that have arisen after the creation of the master OS image. Thus, the image deployment monitor provides dynamic protection to the master OS image by protecting future deployed copies of the master OS image.

Also stored in RAM (168) is an operating system (154). Operating systems useful dynamic protection of a master operating system image according to embodiments of the present invention include UNIX™, Linux™, Microsoft XP™, AIX™, IBM's i5/OS™, and others as will occur to those of skill in the art. The operating system (154) and the image deployment monitor (199) in the example of FIG. 1 are shown in RAM (168), but many components of such software

typically are stored in non-volatile memory also, such as, for example, on a disk drive (170).

The management server (152) of FIG. 1 includes disk drive adapter (172) coupled through expansion bus (160) and bus adapter (158) to processor (156) and other components of the management server (152). Disk drive adapter (172) connects non-volatile data storage to the management server (152) in the form of disk drive (170). Disk drive adapters useful in computers for dynamic protection of a master operating system image according to embodiments of the present invention include Integrated Drive Electronics ('IDE') adapters, Small Computer System Interface ('SCSI') adapters, and others as will occur to those of skill in the art. Non-volatile computer memory also may be implemented for as an optical disk drive, electrically erasable programmable read-only memory (so-called 'EEPROM' or 'Flash' memory), RAM drives, and so on, as will occur to those of skill in the art.

The example management server (152) of FIG. 1 includes one or more input/output ('I/O') adapters (178). I/O adapters implement user-oriented input/output through, for example, software drivers and computer hardware for controlling output to display devices such as computer display screens, as well as user input from user input devices (181) such as keyboards and mice. The example management server (152) of FIG. 1 includes a video adapter (183), which is an example of an I/O adapter specially designed for graphic output to a display device (180) such as a display screen or computer monitor. Video adapter (183) is connected to processor (156) through a high speed video bus (164), bus adapter (158), and the front side bus (162), which is also a high speed bus.

The exemplary management server (152) of FIG. 1 includes a communications adapter (167) for data communications with the repository (189) and other computers, such as client computers (182) via a data communications network (100). Such data communications may be carried out serially through RS-232 connections, through external buses such as a Universal Serial Bus ('USB'), through data communications networks such as IP data communications networks, and in other ways as will occur to those of skill in the art. Communications adapters implement the hardware level of data communications through which one computer sends data communications to another computer, directly or through a data communications network. Examples of communications adapters useful for dynamic protection of a master operating system image according to embodiments of the present invention include modems for wired dial-up communications, Ethernet (IEEE 802.3) adapters for wired data communications network communications, and 802.11 adapters for wireless data communications network communications.

For further explanation, therefore, FIG. 2 sets forth a block diagram of a system comprising another example management server (252) useful in dynamic protection of a master operating system image according to embodiments of the present invention.

The system of FIG. 2 includes a management server (252) with an image deployment monitor (299) configured to monitor a deployed copy (291) of a master OS image. In the example of FIG. 2, a Windows™ master OS image (276) associated with a Windows™ environment (278) and a Linux™ master OS image (246) associated with a Linux™ environment (248) are stored in a master OS image repository (289). Although only two master OS images are shown, any number of other master OS images may be stored in the repository (289). In the example of FIG. 2, only one deployed copy of a master OS image is illustrated but the image deployment monitor (299) may be configured to monitor any number of deployed copies of any number of master OS images.

In the example of FIG. 2, each master OS image (276, 246) has an associated blacklist (280, 260), a default configuration (282, 262), and other meta data (284, 264). A blacklist is a list indicating software modules that have been identified as creating problems on one or more deployed copies of the master OS image. That is, each software module listed in the blacklist has been associated with a negative change in an operational state of a deployed copy of a master OS image. Future deployed copies of a master OS image, upon deployment, use the blacklist to determine which software modules should be prevented from being installed on the future deployed copy. A default configuration is a collection of settings associated with deployment of a copy of a master OS image. For example, a default configuration may indicate how a particular drive is to be partitioned, memory allocated, and CPU and network bandwidth distributed. Other meta data may include rules, procedures, or any other type of information that may relate to deployment and execution of a copy of a master OS image.

During operation, the image deployment monitor (299) may receive one or more alerts (230) from the deployed copy (291) of the master OS image (276) associated with the Windows™ environment (278). An alert may indicate an operational state of the deployed copy (291). Examples of operational states may include a system error or loss of contact with a peripheral device. An alert may also indicate a configuration change in the deployed copy (291). Examples of configuration changes may include installation of a software component, such as a device driver, or modification of a resource allocation, such as changing the size of memory, CPU bandwidth, or network bandwidth.

Based on information within one or more alerts (230), the image deployment monitor (299) may generate a configuration recommendation (232). For example, the image deployment monitor (299) may determine that the deployed copy (291) installed a device driver and shortly afterwards experienced a system crash. In this example, the image deployment monitor (299) may conclude that the installation of the device driver was the cause of the system crash. Based on this conclusion, the configuration recommendation generated by the image deployment monitor (299) may specify an action designed to prevent the crash from occurring in future deployed copies of the master OS image. For example, the configuration recommendation may include an instruction to add the device driver to the blacklist (280) associated with the master OS image (276).

The image deployment monitor (299) may provide the configuration recommendation (232) to a master OS image repository (289) for application to the master OS image (276). For example, a future deployed copy of the master OS image (276), may utilize an adjustment module (274) to examine the blacklist (280), the default configuration (282), and other meta data (284) to determine which installations of software modules to prevent, which hardware and software configurations to apply, and other rules or information associated with deployment. The adjustment module (274) is included in a future deployed copy of the master OS image (276) and is capable of utilizing information gathered from previously deployed copies. That is, the adjustment module (274) is capable of modifying a copy of the master OS image using special instructions or via deployment policy settings.

For further explanation, FIG. 3 sets forth a flow chart illustrating an exemplary method for dynamic protection of a master operating system image according to embodiments of the present invention. The method of FIG. 3 includes monitoring (302), by an image deployment monitor (301), an operational state (350) of a deployed copy (303) of a master

5

operating system (OS) image (394). Monitoring (302) an operational state (350) of a deployed copy (303) of a master operating system (OS) image (394) may be carried out by installing a monitoring agent on the deployed copy. A monitoring agent may be configured to monitor data metrics such as availability and performance of an operating system and specific applications installed on a system associated with the deployed copy. That is, the image deployment monitor may act as a management hub for collecting and reporting on the data metrics gathered by the monitoring agents.

An operational state may be any type of monitorable characteristic related to the deployed copy. For example, an operational state may indicate a physical state of the system upon which the deployed copy resides, such as temperatures, chassis integrity, power supply, and fan speed. As another non-limiting example, an operational state may be related to server performance, such as SNMP monitoring, hard disk utilization, file integrity and size, memory utilization, CPU utilization, cache utilization, and other processes related to server performance. An operational state may be related to performance of a particular service, such as DNS, HTTP, FTP, Telnet, NNTP, SMTP. An operational state may also relate to network monitoring such as network throughput, current logons, failover/cluster monitoring or web site monitoring, such as hit rate, page content verification, database connection verification, and cache rate. Security parameters may also be indicated by an operational state, such as intrusion monitoring and login error monitoring.

The method of FIG. 3 includes detecting (304), by the image deployment monitor (301), a change in the operational state (350) of the deployed copy (303) of the master OS image (394). Non-limiting examples of changes in operational states include system errors or failures related to a particular monitorable characteristic of the deploy copy. Detecting (304), by the image deployment monitor (301), a change in the operational state (350) of the deployed copy (303) of the master OS image (394) may be carried out by receiving from a monitoring agent, an alert indicating a change in the monitored operational state of a deployed copy. For example, an alert may indicate a particular type of system error, a failure to communicate with a virtual peripheral device, or any other type of information related to an operational state.

The method of FIG. 3 includes generating (306) in response to detecting the change, by the image deployment monitor (301), a configuration recommendation (332) to prevent the change from occurring in operational states of future deployed copies of the master OS image (394). Generating (306) in response to detecting the change, a configuration recommendation (332) to prevent the change from occurring in operational states of future deployed copies of the master OS image (394) may be carried out by determining a cause of the change in operational state; identifying a preventative action corresponding to the cause of the change; and specifying the preventative action within the configuration recommendation. For example, if the change in an operational state is determined to be due to addition of a software module, the image deployment monitor (301) may specify within the configuration recommendation, a preventative action designed to prevent installation of the software module in future deployed copies. In this example, the configuration recommendation may indicate a preventative action of adding the software module to a blacklist. As another example, if the change in operational state is due to insufficient resources, such as insufficient network bandwidth, CPU bandwidth, or memory space, the preventative action indicated in the configuration recommendation may specify changing the default configuration of future deployed copies of the master OS

6

image. In this example, the configuration recommendation may change the amount of network bandwidth, CPU bandwidth, or memory space available to the future deployed copies of the master OS image.

The method of FIG. 3 also includes providing (308), by the image deployment monitor (301), the configuration recommendation (332) to the master OS image (394). As explained above, a configuration recommendation is designed to prevent a particular change from occurring in future deployed copies. To accomplish this task, a configuration recommendation may include different types of data. For example, if the configuration recommendation is designed to prevent installation of a particular software component, the configuration recommendation may include data specifying attributes of offending software modules, such as version number, author, and distribution number. Providing (308), by the image deployment monitor (301), the configuration recommendation (332) to the master OS image (394) may be carried out by using direct or indirect communication to communicate with a repository (389) that includes the master OS image (394).

For further explanation, FIG. 4 sets forth a flow chart illustrating a further exemplary method for dynamic protection of a master operating system image according to embodiments of the present invention. The method of FIG. 4 is similar to the method of FIG. 3 in that the method of FIG. 4 also includes monitoring (302) an operational state (350) of a deployed copy (303) of a master operating system (OS) image (394); detecting (304) a change in the operational state (350) of the deployed copy (303) of the master OS image (394); generating (306) in response to detecting the change, a configuration recommendation (332) to prevent the change from occurring in operational states of future deployed copies of the master OS image (394); and providing (308) the configuration recommendation (332) to the master OS image (394).

The method of FIG. 4 also includes detecting (402), by the image deployment monitor (301), a configuration change (450) to the deployed copy (303) of the master OS image (394). A configuration change may be any type of modification to the deployed copy. Examples of configuration changes include installation of a software module, change in a hardware or software setting related to the deployed copy. Detecting (402), by the image deployment monitor (301), a configuration change (450) to the deployed copy (303) of the master OS image (394) may be carried out by receiving from the deployed copy an alert including a change in the configuration of the deployed copy.

In the method of FIG. 4, however, generating (306) in response to detecting the change, a configuration recommendation (332) to prevent the change from occurring in operational states of future deployed copies of the master OS image (394) includes identifying (404) the configuration change (450) as the cause of the change in the operational state (350) of the deployed copy (303) of the master OS image (394). Identifying (404) the configuration change (450) as the cause of the change in the operational state (350) of the deployed copy (303) of the master OS image (394) may be carried out by examining an alert indicating a configuration change; associating a detected change in an operational state with the configuration change; and identifying a preventative action designed to prevent the configuration change in future deployed copies and thus prevent the change in the operational state from occurring in future deployed copies.

That is, the configuration recommendation (450) may prevent the configuration change (450) from occurring in future deployed copies of the master operating system image (394). For example, the configuration change (450) may be associated with installation of a software component to the

deployed copy (303) of the master OS image (394). In this case, the configuration recommendation may prevent the installation of the software component on future deployed copies of the master OS image by adding an identification of the software component to a blacklist associated with the master OS image.

Exemplary embodiments of the present invention are described largely in the context of a fully functional computer system for dynamic protection of a master operating system image. Readers of skill in the art will recognize, however, that the present invention also may be embodied in a computer program product disposed upon computer readable storage media for use with any suitable data processing system. Such computer readable storage media may be any storage medium for machine-readable information, including magnetic media, optical media, or other suitable media. Examples of such media include magnetic disks in hard drives or diskettes, compact disks for optical drives, magnetic tape, and others as will occur to those of skill in the art. Persons skilled in the art will immediately recognize that any computer system having suitable programming means will be capable of executing the steps of the method of the invention as embodied in a computer program product. Persons skilled in the art will recognize also that, although some of the exemplary embodiments described in this specification are oriented to software installed and executing on computer hardware, nevertheless, alternative embodiments implemented as firmware or as hardware are well within the scope of the present invention.

As will be appreciated by one skilled in the art, aspects of the present invention may be embodied as a system, method or computer program product. Accordingly, aspects of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present invention may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable

medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

Aspects of the present invention are described above with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted

in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

It will be understood from the foregoing description that modifications and changes may be made in various embodiments of the present invention without departing from its true spirit. The descriptions in this specification are for purposes of illustration only and are not to be construed in a limiting sense. The scope of the present invention is limited only by the language of the following claims.

What is claimed is:

1. An apparatus for dynamic protection of a master operating system image, the apparatus comprising a computer processor, a computer memory operatively coupled to the computer processor, the computer memory having disposed within it computer program instructions that, when executed by the computer processor, cause the apparatus to carry out the steps of:

detecting, by an image deployment monitor, a configuration change to a deployed copy of a master operating system ('OS') image;

detecting, by the image deployment monitor, a change in an operational state of the deployed copy of the master OS image;

in response to detecting the change, generating, by the image deployment monitor, a configuration recommendation to prevent the change from occurring in operational states of future deployed copies of the master OS image, including identifying the configuration change as the cause of the change in the operational state of the deployed copy of the master OS image, wherein the configuration recommendation comprises a recommendation to modify a resource allocation; and

in response to identifying the configuration change as the cause of the change in the operational state of the deployed copy of the master OS image, modifying the master OS image to prevent the configuration change from occurring in future deployed copies of the master OS image, wherein modifying the master OS image comprises modifying the resource allocation and wherein the master OS image includes an adjustment module configured to modify the master OS image based on the configuration recommendation.

2. The apparatus of claim 1 wherein the configuration recommendation prevents the configuration change from occurring in future deployed copies of the master operating system image.

3. The apparatus of claim 2 wherein the configuration change is associated with installation of a software component to the deployed copy of the master OS image; and wherein the configuration recommendation prevents the

installation of the software component on future deployed copies of the master OS image.

4. The apparatus of claim 1 wherein the adjustment module is further configured to modify future deployed copies of the master OS image based on the configuration recommendation.

5. The apparatus of claim 1 wherein the image deployment monitor is located on a management server; wherein the deployed copy of the master OS image is located on a client system.

6. A computer program product for dynamic protection of a master operating system image, the computer program product disposed upon a non-transitory computer readable medium, wherein the computer readable medium is not a signal, the computer program product comprising computer program instructions that, when executed, cause a computer to carry out the steps of:

detecting, by an image deployment monitor, a configuration change to a deployed copy of a master operating system ('OS') image;

detecting, by the image deployment monitor, a change in an operational state of the deployed copy of the master OS image;

in response to detecting the change, generating, by the image deployment monitor, a configuration recommendation to prevent the change from occurring in operational states of future deployed copies of the master OS image, including identifying the configuration change as the cause of the change in the operational state of the deployed copy of the master OS image, wherein the configuration recommendation comprises a recommendation to modify a resource allocation; and

in response to identifying the configuration change as the cause of the change in the operational state of the deployed copy of the master OS image, modifying the master OS image to prevent the configuration change from occurring in future deployed copies of the master OS image, wherein modifying the master OS image comprises modifying the resource allocation and wherein the master OS image includes an adjustment module configured to modify the master OS image based on the configuration recommendation.

7. The computer program product of claim 6 wherein the configuration recommendation prevents the configuration change from occurring in future deployed copies of the master operating system image.

8. The computer program product of claim 7 wherein the configuration change is associated with installation of a software component to the deployed copy of the master OS image; and wherein the configuration recommendation prevents the installation of the software component on future deployed copies of the master OS image.

9. The computer program product of claim 6 wherein the image deployment monitor is located on a management server; wherein the deployed copy of the master OS image is located on a client system.

* * * * *